Hinojosa	McKeon	Salazar
Hobson	McMorris Rodgers	Sánchez, Linda T.
Hoekstra	McNulty	Sanchez, Loretta
Holden	Meek (FL)	Sanders
Holt	Meeks (NY)	Saxton
Honda	Melancon	Schiff
Hooley	Mica	Schmidt
Hostettler	Miller (FL)	Schwartz (PA)
Hoyer	Miller (MI)	Schwarz (MI)
Hulshof	Miller (NC)	Scott (GA)
Hunter	Miller, Gary	Scott (VA)
Hyde	Miller, George	Sensenbrenner
Inglis (SC)	Mollohan	Serrano
Inslee	Moore (KS)	Sessions
Israel	Moran (KS)	Shadegg
Issa	Moran (VA)	Shaw
Jackson (IL)	Murphy	Shays
Jenkins	Murtha	Sherman
Jindal	Musgrave	Sherwood
Johnson (CT)	Myrick	Shimkus
Johnson (IL)	Nadler	Shuster
Johnson, E. B.	Napolitano	Simmons
Johnson, Sam	Neal (MA)	Simpson
Jones (NC)	Neugebauer	Skelton
Jones (OH)	Northup	Slaughter
Kanjorski	Norwood	Smith (NJ)
Kaptur	Nunes	Smith (TX)
Keller	Nussle	Smith (WA)
Kelly	Oberstar	Snyder
Kennedy (MN)	Obey	Sodrel
Kennedy (RI)	Olver	Solis
Kildee	Ortiz	Souder
Kilpatrick (MI)	Osborne	Spratt
Kind	Otter	Stearns
King (IA)	Oxley	Stupak
King (NY)	Pallone	Sullivan
Kingston	Pascrell	Sweeney
Kirk	Pearce	Tancredo
Kline	Pelosi	Tanner
Knollenberg	Pence	Tauscher
Kolbe	Peterson (MN)	Taylor (MS)
Kuhl (NY)	Peterson (PA)	Taylor (NC)
LaHood	Petri	Terry
Langevin	Pickering	Thompson (CA)
Lantos	Pitts	Thompson (MS)
Larsen (WA)	Platts	Thornberry
Larson (CT)	Poe	Tiahrt
Latham	Pomeroy	Tiberi
LaTourette	Porter	Tierney
Leach	Price (GA)	Towns
Levin	Price (NC)	Turner
Lewis (CA)	Pryce (OH)	Udall (CO)
Lewis (KY)	Putnam	Udall (NM)
Linder	Radanovich	Upton
Lipinski	Rahall	Van Hollen
LoBiondo	Ramstad	Visclosky
Lofgren, Zoe	Regula	Walden (OR)
Lowey	Rehberg	Walsh
Lucas	Reichert	Wamp
Lungren, Daniel E.	Renzi	Wasserman Schultz
Lynch	Reyes	Watson
Mack	Reynolds	Weiner
Maloney	Rogers (AL)	Weldon (FL)
Manzullo	Rogers (KY)	Weldon (PA)
Marchant	Rogers (MI)	Weller
Markey	Rohrabacher	Westmoreland
Marshall	Ros-Lehtinen	Wexler
Matheson	Ross	Whitfield
Matsui	Rothman	Wicker
McCarthy	Roybal-Allard	Wilson (NM)
McCaul (TX)	Royce	Wilson (SC)
McCollum (MN)	Ruppersberger	Wolf
McCotter	Rush	Wu
McGovern	Ryan (OH)	Wynn
McHenry	Ryan (WI)	Young (AK)
McHugh	Ryun (KS)	Young (FL)
McIntyre	Sabo	

NAYS—22

Baldwin	Lee	Rangel
Conyers	McDermott	Schakowsky
Duncan	McKinney	Stark
Filner	Michaud	Velázquez
Frank (MA)	Moore (WI)	Waters
Jackson-Lee (TX)	Owens	Watt
Kucinich	Paul	Woolsey
	Payne	

NOT VOTING—16

Boehlert	Lewis (GA)	Pastor
Castle	McCrery	Pombo
Davis (FL)	Meehan	Strickland
Evans	Millender-McDonald	Thomas
Istook	Ney	Waxman
Jefferson		

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore (during the vote). Members are advised there is 1 minute remaining in this vote.

□ 2146

So the conference report was agreed to.

The result of the vote was announced as above recorded.

A motion to reconsider was laid on the table.

Stated for:

Mr. MCCRERY. Mr. Speaker, on rollcall No. 486 I was unavoidably detained. Had I been present, I would have voted "yea."

Mr. JEFFERSON. Mr. Speaker, I am in favor of the conference report and I thank the Defense appropriations subcommittee for its hard work. Had I been present for the vote, I would have voted "yea."

ANNOUNCEMENT BY THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX, the Chair will postpone further proceedings today on motions to suspend the rules on which a recorded vote or the yeas and nays are ordered, or on which the vote is objected to under clause 6 of rule XX.

Record votes on postponed questions will be taken tomorrow.

VETERANS IDENTITY AND CREDIT SECURITY ACT OF 2006

Mr. BUYER. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5835) to amend title 38, United States Code, to improve information management within the Department of Veterans Affairs, and for other purposes, as amended.

The Clerk read as follows:

H.R. 5835

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Veterans Identity and Credit Security Act of 2006''.

SEC. 2. FEDERAL AGENCY DATA BREACH NOTIFICATION REQUIREMENTS.

(a) AUTHORITY OF DIRECTOR OF OFFICE OF MANAGEMENT AND BUDGET TO ESTABLISH DATA BREACH POLICIES.—Section 3543(a) of title 44, United States Code, is amended—

(1) by striking ''and'' at the end of paragraph (7);

(2) by striking the period and inserting ''; and'' at the end of paragraph (8); and

(3) by adding at the end the following:

''(9) establishing policies, procedures, and standards for agencies to follow in the event of a breach of data security involving the disclosure of sensitive personal information and for which harm to an individual could reasonably be expected to result, specifically including—

''(A) a requirement for timely notice to be provided to those individuals whose sensitive personal information could be compromised as a result of such breach, except no notice shall be required if the breach does not create a reasonable risk of identity theft, fraud, or other unlawful conduct regarding such individual;

''(B) guidance on determining how timely notice is to be provided; and

''(C) guidance regarding whether additional special actions are necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services.''.

(b) AUTHORITY OF CHIEF INFORMATION OFFICER TO ENFORCE DATA BREACH POLICIES AND DEVELOP AND MAINTAIN INVENTORIES.—Section 3544(a)(3) of title 44, United States Code, is amended—

(1) by inserting after ''authority to ensure compliance with'' the following: ''and, to the extent determined necessary and explicitly authorized by the head of the agency, to enforce'';

(2) by striking ''and'' at the end of subparagraph (D);

(3) by inserting ''and'' at the end of subparagraph (E); and

(4) by adding at the end the following:

''(F) developing and maintaining an inventory of all personal computers, laptops, or any other hardware containing sensitive personal information;''.

(c) INCLUSION OF DATA BREACH NOTIFICATION IN AGENCY INFORMATION SECURITY PROGRAMS.—Section 3544(b) of title 44, United States Code, is amended—

(1) by striking ''and'' at the end of paragraph (7);

(2) by striking the period and inserting ''; and'' at the end of paragraph (8); and

(3) by adding at the end the following:

''(9) procedures for notifying individuals whose sensitive personal information is compromised consistent with policies, procedures, and standards established under section 3543(a)(9) of this title.''.

(d) AUTHORITY OF AGENCY CHIEF HUMAN CAPITAL OFFICERS TO ASSESS FEDERAL PERSONAL PROPERTY.—Section 1402(a) of title 5, United States Code, is amended—

(1) by striking '', and'' at the end of paragraph (5) and inserting a semicolon;

(2) by striking the period and inserting ''; and'' at the end of paragraph (6); and

(3) by adding at the end the following:

''(7) prescribing policies and procedures for exit interviews of employees, including a full accounting of all Federal personal property that was assigned to the employee during the course of employment.''.

(e) SENSITIVE PERSONAL INFORMATION DEFINITION.—Section 3542(b) of title 44, United States Code, is amended by adding at the end the following new paragraph:

''(4) The term 'sensitive personal information', with respect to an individual, means any information about the individual maintained by an agency, including—

''(A) education, financial transactions, medical history, and criminal or employment history;

''(B) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records; or

''(C) any other personal information that is linked or linkable to the individual.''.

SEC. 3. UNDER SECRETARY FOR INFORMATION SERVICES.

(a) UNDER SECRETARY.—Chapter 3 of title 38, United States Code, is amended by inserting after section 307 the following new section:

''§ 307A. Under Secretary for Information Services

''(a) UNDER SECRETARY.—There is in the Department an Under Secretary for Information Services, who is appointed by the President, by and with the advice and consent of the Senate. The Under Secretary shall be the head of the Office of Information Services and shall perform such functions as the Secretary shall prescribe.

''(b) SERVICE AS CHIEF INFORMATION OFFICER.—Notwithstanding any other provision of law, the Under Secretary for Information Services shall serve as the Chief Information Officer of the Department under section 310 of this title.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by inserting after the item relating to section 307 the following new item:

''307A. Under Secretary for Information Services.''.

(c) CONFORMING AMENDMENT.—Section 308(b) of such title is amended by striking paragraph (5) and redesignating paragraphs (6) through (11) as paragraphs (5) through (10), respectively.

SEC. 4. DEPARTMENT OF VETERANS AFFAIRS INFORMATION SECURITY.

(a) INFORMATION SECURITY.—Chapter 57 of title 38, United States Code, is amended by adding at the end the following new subchapter:

''SUBCHAPTER III—INFORMATION SECURITY

''§ 5721. Definitions

''For the purposes of this subchapter:

''(1) The term 'sensitive personal information', with respect to an individual, means any information about the individual maintained by an agency, including—

''(A) education, financial transactions, medical history, and criminal or employment history;

''(B) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records; or

''(C) any other personal information that is linked or linkable to the individual.

''(2) The term 'data breach' means the loss, theft, or other unauthorized access to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

''(3) The term 'data breach analysis' means the identification of any misuse of sensitive personal information involved in a data breach.

''(4) The term 'fraud resolution services' means services to assist an individual in the process of recovering and rehabilitating the credit of the individual after the individual experiences identity theft.

''(5) The term 'identity theft' has the meaning given such term under section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

''(6) The term 'identity theft insurance' means any insurance policy that pays benefits for costs, including travel costs, notary fees, and postage costs, lost wages, and legal fees and expenses associated with the identity theft of the insured individual.

''(7) The term 'principal credit reporting agency' means a consumer reporting agency as described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

''§ 5722. Office of the Under Secretary for Information Services

''(a) DEPUTY UNDER SECRETARIES.—The Office of the Under Secretary for Information Services shall consist of the following:

''(1) The Deputy Under Secretary for Information Services for Security, who shall serve as the Senior Information Security Officer of the Department.

''(2) The Deputy Under Secretary for Information Services for Operations and Management.

''(3) The Deputy Under Secretary for Information Services for Policy and Planning.

''(b) APPOINTMENTS.—Appointments under subsection (a) shall be made by the Secretary, notwithstanding the limitations of section 709 of this title.

''(c) QUALIFICATIONS.—At least one of positions established and filled under subsection (a) shall be filled by an individual who has at least five years of continuous service in the Federal civil service in the executive branch immediately preceding the appointment of the individual as a Deputy Under Secretary. For purposes of determining such continuous service of an individual, there shall be excluded any service by such individual in a position—

''(1) of a confidential, policy-determining, policy-making, or policy-advocating character;

''(2) in which such individual served as a noncareer appointee in the Senior Executive Service, as such term is defined in section 3132(a)(7) of title 5; or

''(3) to which such individual was appointed by the President.

''§ 5723. Information security management

''(a) RESPONSIBILITIES OF CHIEF INFORMATION OFFICER.—To support the economical, efficient, and effective execution of subtitle III of chapter 35 of title 44, and policies and plans of the Department, the Secretary shall ensure that the Chief Information Officer of the Department has the authority and control necessary to develop, approve, implement, integrate, and oversee the policies, procedures, processes, activities, and systems of the Department relating to that subtitle, including the management of all related mission applications, information resources, personnel, and infrastructure.

''(b) ANNUAL COMPLIANCE REPORT.—Not later than March 1 of each year, the Secretary shall submit to the Committees on Veterans' Affairs of the Senate and House of Representatives, the Committee on Government Reform of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate, a report on the Department's compliance with subtitle III of chapter 35 of title 44. The information in such report shall be displayed in the aggregate and separately for each Administration, office, and facility of the Department.

''(c) REPORTS TO SECRETARY OF COMPLIANCE DEFICIENCIES.—(1) At least once every month, the Chief Information Officer shall report to the Secretary any deficiency in the compliance with subtitle III of chapter 35 of title 44 of the Department or any Administration, office, or facility of the Department.

''(2) The Chief Information Officer shall immediately report to the Secretary any significant deficiency in such compliance.

''(d) DATA BREACHES.—(1) The Chief Information Officer shall immediately provide notice to the Secretary of any data breach.

''(2) Immediately after receiving notice of a data breach under paragraph (1), the Secretary shall provide notice of such breach to the Director of the Office of Management and Budget, the Inspector General of the Department, and, if appropriate, the Federal Trade Commission and the United States Secret Service.

''(e) BUDGETARY MATTERS.—When the budget for any fiscal year is submitted by the President to Congress under section 1105 of title 31, the Secretary shall submit to Congress a report that identifies amounts requested for Department implementation and remediation of and compliance with this subchapter and subtitle III of chapter 35 of title 44. The report shall set forth those amounts both for each Administration within the Department and for the Department in the aggregate and shall identify, for each such amount, how that amount is aligned with and supports such implementation and compliance.

''§ 5724. Congressional reporting and notification of data breaches

''(a) QUARTERLY REPORTS.—(1) Not later than 30 days after the last day of a fiscal quarter, the Secretary shall submit to the Committees on Veterans' Affairs of the Senate and House of Representatives a report on any data breach with respect to sensitive personal information processed or maintained by the Department that occurred during that quarter.

''(2) Each report submitted under paragraph (1) shall identify, for each data breach covered by the report, the Administration and facility of the Department responsible for processing or maintaining the sensitive personal information involved in the data breach.

''(b) NOTIFICATION OF SIGNIFICANT DATA BREACHES.—(1) In the event of a data breach with respect to sensitive personal information processed or maintained by the Secretary that the Secretary determines is significant, the Secretary shall provide notice of such breach to the Committees on Veterans' Affairs of the Senate and House of Representatives.

''(2) Notice under paragraph (1) shall be provided promptly following the discovery of such a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

''§ 5725. Data breaches

''(a) INDEPENDENT RISK ANALYSIS.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non-Department entity conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

''(2) If the Secretary determines, based on the findings of a risk analysis conducted under paragraph (1), that a reasonable risk exists for the potential misuse of sensitive information involved in a data breach, the Secretary shall provide credit protection services in accordance with section 5726 of this title.

''(b) NOTIFICATION.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall provide to an individual whose sensitive personal information is involved in that breach notice of the data breach—

''(A) in writing; or

''(B) by email, if—

''(i) the Department's primary method of communication with the individual is by email; and

''(ii) the individual has consented to receive such notification.

''(2) Notice provided under paragraph (1) shall—

''(A) describe the circumstances of the data breach and the risk that the breach could lead to misuse, including identity theft, involving the sensitive personal information of the individual;

''(B) describe the specific types of sensitive personal information that was compromised as a part of the data breach;

''(C) describe the actions the Department is taking to remedy the data breach;

''(D) inform the individual that the individual may request a fraud alert and credit security freeze under this section;

''(E) clearly explain the advantages and disadvantages to the individual of receiving

fraud alerts and credit security freezes under this section; and

''(F) includes such other information as the Secretary determines is appropriate.

''(3) The notice required under paragraph (1) shall be provided promptly following the discovery of a data breach and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

''(c) REPORT.—For each data breach with respect to sensitive personal information processed or maintained by the Secretary, the Secretary shall promptly submit to the Committees on Veterans' Affairs of the Senate and House of Representatives a report containing the findings of any independent risk analysis conducted under subsection (a)(1), any determination of the Secretary under subsection (a)(2), and a description of any credit protection services provided under section 5726 of this title.

''(d) FINAL DETERMINATION.—Notwithstanding sections 511 and 7104(a) of this title, any determination of the Secretary under subsection (a)(2) with respect to the reasonable risk for the potential misuse of sensitive information involved in a data breach is final and conclusive and may not be reviewed by any other official, administrative body, or court, whether by an action in the nature of mandamus or otherwise.

''(e) FRAUD ALERTS.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall arrange, upon the request of an individual whose sensitive personal information is involved in the breach to a principal credit reporting agency with which the Secretary has entered into a contract under section 5726(d) and at no cost to the individual, for the principal credit reporting agency to provide fraud alert services for that individual for a period of not less than one year, beginning on the date of such request, unless the individual requests that such fraud alert be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

''(2) The Secretary shall arrange for each principal credit reporting agency referred to in paragraph (1) to provide any alert requested under such subsection in the file of the individual along with any credit score generated in using that file, for a period of not less than one year, beginning on the date of such request, unless the individual requests that such fraud alert be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

''(f) CREDIT SECURITY FREEZE.—(1) In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall arrange, upon the request of an individual whose sensitive personal information is involved in the breach and at no cost to the individual, for each principal credit reporting agency to apply a security freeze to the file of that individual for a period of not less than one year, beginning on the date of such request, unless the individual requests that such security freeze be removed before the end of such period, and the agency receives appropriate proof of the identity of the individual for such purpose.

''(2) The Secretary shall arrange for a principal credit reporting agency applying a security freeze under paragraph (1)—

''(A) to send a written confirmation of the security freeze to the individual within five business days of applying the freeze;

''(B) to refer the information regarding the security freeze to other consumer reporting agencies;

''(C) to provide the individual with a unique personal identification number or password to be used by the individual when providing authorization for the release of the individual's credit for a specific party or period of time; and

''(D) upon the request of the individual, to temporarily lift the freeze for a period of time specified by the individual, beginning not later than three business days after the date on which the agency receives the request.

''§ 5726. Provision of credit protection services

''(a) COVERED INDIVIDUAL.—For purposes of this section, a covered individual is an individual whose sensitive personal information that is processed or maintained by the Department (or any third-party entity acting on behalf of the Department) is involved, on or after August 1, 2005, in a data breach for which the Secretary determines a reasonable risk exists for the potential misuse of sensitive personal information under section 5725(a)(2) of this title.

''(b) NOTIFICATION.—(1) In addition to any notice required under subsection 5725(b) of this title, the Secretary shall provide to a covered individual notice in writing that—

''(A) the individual may request credit protection services under this section;

''(B) clearly explains the advantages and disadvantages to the individual of receiving credit protection services under this section;

''(E) includes a notice of which principal credit reporting agency the Secretary has entered into a contract with under subsection (d), and information about requesting services through that agency;

''(C) describes actions the individual can or should take to reduce the risk of identity theft; and

''(D) includes such other information as the Secretary determines is appropriate.

''(2) The notice required under paragraph (1) shall be made as promptly as possible and without unreasonable delay following the discovery of a data breach for which the Secretary determines a reasonable risk exists for the potential misuse of sensitive personal information under section 5725(a)(2) of this title and the implementation of any measures necessary to determine the scope of the breach, prevent any further breach or unauthorized disclosures, and reasonably restore the integrity of the data system.

''(3) The Secretary shall ensure that each notification under paragraph (1) includes a form or other means for readily requesting the credit protection services under this section. Such form or other means may include a telephone number, email address, or Internet website address.

''(c) AVAILABILITY OF SERVICES THROUGH OTHER GOVERNMENT AGENCIES.—If a service required to be provided under this section is available to a covered individual through another department or agency of the Government, the Secretary and the head of that department or agency may enter into an agreement under which the head of that department or agency agrees to provide that service to the covered individual.

''(d) CONTRACT WITH CREDIT REPORTING AGENCY.—Subject to the availability of appropriations and notwithstanding any other provision of law, the Secretary shall enter into contracts or other agreements as necessary with one or more principal credit reporting agencies in order to ensure, in advance, the provision of credit protection services under this section and fraud alerts and security freezes under section 5725 of this title. Any such contract or agreement may include provisions for the Secretary to pay the expenses of such a credit reporting agency for the provision of such services.

''(e) DATA BREACH ANALYSIS.—The Secretary shall arrange, upon the request of a covered individual and at no cost to the individual, to provide data breach analysis for the individual for a period of not less than one year, beginning on the date of such request.

''(f) PROVISION OF CREDIT MONITORING SERVICES AND IDENTITY THEFT INSURANCE.—During the one-year period beginning on the date on which the Secretary notifies a covered individual that the individual's sensitive personal information is involved in a data breach, the Secretary shall arrange, upon the request of the individual and without charge to the individual, for the provision of credit monitoring services to the individual. Credit monitoring services under this subsection shall include each of the following:

''(1) One copy of the credit report of the individual every three months.

''(2) Fraud resolution services for the individual.

''(3) Identity theft insurance in a coverage amount that does not exceed $30,000 in aggregate liability for the insured.

''§ 5727. Contracts for data processing or maintenance

''(a) CONTRACT REQUIREMENTS.—If the Secretary enters into a contract for the performance of any Department function that requires access to sensitive personal information, the Secretary shall require as a condition of the contract that—

''(1) the contractor shall not, directly or through an affiliate of the contractor, disclose such information to any other person unless the disclosure is lawful and is expressly permitted under the contract;

''(2) the contractor, or any subcontractor for a subcontract of the contract, shall promptly notify the Secretary of any data breach that occurs with respect to such information.

''(b) LIQUIDATED DAMAGES.—Each contract subject to the requirements of subsection (a) shall provide for liquidated damages to be paid by the contractor to the Secretary in the event of a data breach with respect to any sensitive personal information processed or maintained by the contractor or any subcontractor under that contract.

''(c) PROVISION OF CREDIT PROTECTION SERVICES.—Any amount collected by the Secretary under subsection (b) shall be deposited in or credited to the Department account from which the contractor was paid and shall remain available for obligation without fiscal year limitation exclusively for the purpose of providing credit protection services in accordance with section 5726 of this title.

''§ 5728. Authorization of appropriations

''There are authorized to be appropriated to carry out this subchapter such sums as may be necessary for each fiscal year.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by adding at the end the following new items:

''SUBCHAPTER III—INFORMATION SECURITY

''5721. Definitions.
''5722. Office of the Under Secretary for Information Services.
''5723. Information security management.
''5724. Congressional reporting and notification of data breaches.
''5725. Data breaches.
''5726. Provision of credit protection services.
''5727. Contracts for data processing or maintenance.
''5728. Authorization of appropriations.''.

(c) DEADLINE FOR REGULATIONS.—Not later than 60 days after the date of the enactment

of this Act, the Secretary of Veterans Affairs shall publish regulations to carry out subchapter III of chapter 57 of title 38, United States Code, as added by subsection (a).

SEC. 5. REPORT ON FEASIBILITY OF USING PERSONAL IDENTIFICATION NUMBERS FOR IDENTIFICATION.

Not later than 180 days after the date of the enactment of this Act, the Secretary of Veterans Affairs shall submit to Congress a report containing the assessment of the Secretary with respect to the feasibility of using personal identification numbers instead of Social Security numbers for the purpose of identifying individuals whose sensitive personal information (as that term is defined in section 5721 of title 38, United States Code, as added by section 4) is processed or maintained by the Secretary.

SEC. 6. DEADLINE FOR APPOINTMENTS.

(a) DEADLINE.—Not later than 180 days after the date of the enactment of this Act—

(1) the President shall nominate an individual to serve as the Under Secretary of Veterans Affairs for Information Services under section 307A of title 38, United States Code, as added by section 3; and

(2) the Secretary of Veterans Affairs shall appoint an individual to serve as each of the Deputy Under Secretaries of Veterans Affairs for Information Services under section 5722 of such title, as added by section 4.

(b) REPORT.—Not later than 30 days after the date of the enactment of this Act, and every 30 days thereafter until the appointments described in subsection (a) are made, the Secretary of Veterans Affairs shall submit to Congress a report describing the progress of such appointments.

SEC. 7. INFORMATION SECURITY EDUCATION ASSISTANCE PROGRAM.

(a) PROGRAM REQUIRED.—Title 38, United States Code, is amended by inserting after chapter 78 the following new chapter:

"CHAPTER 79—INFORMATION SECURITY EDUCATION ASSISTANCE PROGRAM

"§ 7901. Programs; purpose

''(a) IN GENERAL.—To encourage the recruitment and retention of Department personnel who have the information security skills necessary to meet Department requirements, the Secretary shall carry out programs in accordance with this chapter to provide financial support for education in computer science and electrical and computer engineering at accredited institutions of higher education.

''(b) TYPES OF PROGRAMS.—The programs authorized under this chapter are as follows:

''(1) Scholarships for pursuit of doctoral degrees in computer science and electrical and computer engineering at accredited institutions of higher education.

''(2) Education debt reduction for Department personnel who hold doctoral degrees in computer science and electrical and computer engineering at accredited institutions of higher education.

"§ 7902. Scholarship program

''(a) AUTHORITY.—(1) Subject to the availability of appropriations, the Secretary shall establish a scholarship program under which the Secretary shall, subject to subsection (d), provide financial assistance in accordance with this section to a qualified person—

''(A) who is pursuing a doctoral degree in computer science or electrical or computer engineering at an accredited institution of higher education; and

''(B) who enters into an agreement with the Secretary as described in subsection (b).

''(2)(A) Except as provided under subparagraph (B), the Secretary may provide financial assistance under this section to an individual for up to five years.

''(B) The Secretary may waive the limitation under subparagraph (A) if the Secretary determines that such a waiver is appropriate.

''(3)(A) The Secretary may award up to five scholarships for any academic year to individuals who did not receive assistance under this section for the preceding academic year.

''(B) Not more than one scholarship awarded under subparagraph (A) may be awarded to an individual who is an employee of the Department when the scholarship is awarded.

''(b) SERVICE AGREEMENT FOR SCHOLARSHIP RECIPIENTS.—(1) To receive financial assistance under this section an individual shall enter into an agreement to accept and continue employment in the Department for the period of obligated service determined under paragraph (2).

''(2) For the purposes of this subsection, the period of obligated service for a recipient of financial assistance under this section shall be the period determined by the Secretary as being appropriate to obtain adequate service in exchange for the financial assistance and otherwise to achieve the goals set forth in section 7901(a) of this title. In no event may the period of service required of a recipient be less than the period equal to two times the total period of pursuit of a degree for which the Secretary agrees to provide the recipient with financial assistance under this section. The period of obligated service is in addition to any other period for which the recipient is obligated to serve on active duty or in the civil service, as the case may be.

''(3) An agreement entered into under this section by a person pursuing an doctoral degree shall include terms that provide the following:

''(A) That the period of obligated service begins on a date after the award of the degree that is determined under the regulations prescribed under section 7906 of this title.

''(B) That the individual will maintain satisfactory academic progress, as determined in accordance with those regulations, and that failure to maintain such progress constitutes grounds for termination of the financial assistance for the individual under this section.

''(C) Any other terms and conditions that the Secretary determines appropriate for carrying out this section.

''(c) AMOUNT OF ASSISTANCE.—(1) The amount of the financial assistance provided for an individual under this section shall be the amount determined by the Secretary as being necessary to pay—

''(A) the tuition and fees of the individual; and

''(B) $1500 to the individual each month (including a month between academic semesters or terms leading to the degree for which such assistance is provided or during which the individual is not enrolled in a course of education but is pursuing independent research leading to such degree) for books, laboratory expenses, and expenses of room and board.

''(2) In no case may the amount of assistance provided for an individual under this section for an academic year exceed $50,000.

''(3) In no case may the total amount of assistance provided for an individual under this section exceed $200,000.

''(4) Notwithstanding any other provision of law, financial assistance paid an individual under this section shall not be considered as income or resources in determining eligibility for, or the amount of benefits under, any Federal or federally assisted program.

''(d) REPAYMENT FOR PERIOD OF UNSERVED OBLIGATED SERVICE.—(1) An individual who receives financial assistance under this section shall repay to the Secretary an amount equal to the unearned portion of the financial assistance if the individual fails to satisfy the requirements of the service agreement entered into under subsection (b), except in certain circumstances authorized by the Secretary.

''(2) The Secretary may establish, by regulations, procedures for determining the amount of the repayment required under this subsection and the circumstances under which an exception to the required repayment may be granted.

''(3) An obligation to repay the Secretary under this subsection is, for all purposes, a debt owed the United States. A discharge in bankruptcy under title 11 does not discharge a person from such debt if the discharge order is entered less than five years after the date of the termination of the agreement or contract on which the debt is based.

''(e) WAIVER OR SUSPENSION OF COMPLIANCE.—The Secretary shall prescribe regulations providing for the waiver or suspension of any obligation of a individual for service or payment under this section (or an agreement under this section) whenever noncompliance by the individual is due to circumstances beyond the control of the individual or whenever the Secretary determines that the waiver or suspension of compliance is in the best interest of the United States.

''(f) INTERNSHIPS.—(1) The Secretary may offer a compensated internship to an individual for whom financial assistance is provided under this section during a period between academic semesters or terms leading to the degree for which such assistance is provided. Compensation provided for such an internship shall be in addition to the financial assistance provided under this section.

''(2) An internship under this subsection shall not be counted toward satisfying a period of obligated service under this section.

''(g) INELIGIBILITY OF INDIVIDUALS RECEIVING MONTGOMERY GI BILL EDUCATION ASSISTANCE PAYMENTS.—An individual who receives a payment of educational assistance under chapter 30, 31, 32, 34, or 35 of this title or chapter 1606 or 1607 of title 10 for a month in which the individual is enrolled in a course of education leading to a doctoral degree in information security is not eligible to receive financial assistance under this section for that month.

"§ 7903. Education debt reduction program

''(a) AUTHORITY.—(1) Subject to the availability of appropriations, the Secretary shall establish an education debt reduction program under which the Secretary shall make education debt reduction payments under this section to qualified individuals eligible under subsection (b) for the purpose of reimbursing such individuals for payments by such individuals of principal and interest on loans described in paragraph (2) of that subsection.

''(2)(A) For each fiscal year, the Secretary may accept up to five individuals into the program established under paragraph (1)who did not receive such a payment during the preceding fiscal year.

''(B) Not more than one individual accepted into the program for a fiscal year under subsection (A) shall be a Department employee as of the date on which the individual is accepted into the program.

''(b) ELIGIBILITY.—An individual is eligible to participate in the program under this section if the individual—

''(1) has completed a doctoral degree a doctoral degree in computer science or electrical or computer engineering at an accredited institution of higher education during the five-year period preceding the date on which the individual is hired;

''(2) is an employee of the Department who serves in a position related to information security (as determined by the Secretary); and

''(3) owes any amount of principal or interest under a loan, the proceeds of which were used by or on behalf of that individual to pay costs relating to a doctoral degree in computer science or electrical or computer engineering at an accredited institution of higher education.

''(c) AMOUNT OF ASSISTANCE.—(1) Subject to paragraph (2), the amount of education debt reduction payments made to an individual under this section may not exceed $82,500 over a total of five years, of which not more than $16,500 of such payments may be made in each year.

''(2) The total amount payable to an individual under this section for any year may not exceed the amount of the principal and interest on loans referred to in subsection (b)(3) that is paid by the individual during such year.

''(d) PAYMENTS.—(1) The Secretary shall make education debt reduction payments under this section on an annual basis.

''(2) The Secretary shall make such a payment—

''(A) on the last day of the one-year period beginning on the date on which the individual is accepted into the program established under subsection (a); or

''(B) in the case of an individual who received a payment under this section for the preceding fiscal year, on the last day of the one-year period beginning on the date on which the individual last received such a payment.

''(3) Notwithstanding any other provision of law, education debt reduction payments under this section shall not be considered as income or resources in determining eligibility for, or the amount of benefits under, any Federal or federally assisted program.

''(e) PERFORMANCE REQUIREMENT.—The Secretary may make education debt reduction payments to an individual under this section for a year only if the Secretary determines that the individual maintained an acceptable level of performance in the position or positions served by the individual during the year.

''(f) NOTIFICATION OF TERMS OF PROVISION OF PAYMENTS.—The Secretary shall provide to an individual who receives a payment under this section notice in writing of the terms and conditions that apply to such a payment.

''(g) COVERED COSTS.—For purposes of subsection (b)(3), costs relating to a course of education or training include—

''(1)) tuition expenses; and

''(2) all other reasonable educational expenses, including fees, books, and laboratory expenses;

''§ 7904. Preferences in awarding financial assistance

''In awarding financial assistance under this chapter, the Secretary shall give a preference to qualified individuals who are otherwise eligible to receive the financial assistance in the following order of priority:

''(1) Veterans with service-connected disabilities.

''(2) Veterans.

''(3) Persons described in section 4215(a)(B) of this title.

''(4) Individuals who received or are pursuing degrees at institutions designated by the National Security Agency as Centers of Academic Excellence in Information Assurance Education.

''(5) Citizens of the United States.

''§ 7905. Requirement of honorable discharge for veterans receiving assistance

''No veteran shall receive financial assistance under this chapter unless the veteran was discharged from the Armed Forces under honorable conditions.

''§ 7906. Regulations

''The Secretary shall prescribe regulations for the administration of this chapter.

''§ 7907. Termination

''The authority of the Secretary to make a payment under this chapter shall terminate on July 31, 2017.''.

(b) GAO REPORT.—Not later than three years after the date of the enactment of this Act, the Comptroller General shall submit to Congress a report on the scholarship and education debt reduction programs under chapter 79 of title 38, United States Code, as added by subsection (a).

(c) APPLICABILITY OF SCHOLARSHIPS.—Section 7902 of title 38, United States Code, as added by subsection (a), shall apply with respect to financial assistance provided for an academic semester or term that begins on or after August 1, 2007.

(d) CLERICAL AMENDMENT.—The tables of chapters at the beginning of such title, and at the beginning of part V of such title, are amended by inserting after the item relating to chapter 78 the following new item:

''79. Information Security Education Assistance Program ..... 7901''.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Indiana (Mr. BUYER) and the gentleman from California (Mr. FILNER) each will control 20 minutes.

The Chair recognizes the gentleman from Indiana.

Mr. BUYER. Mr. Speaker, as chairman of the Committee on Veterans' Affairs, I rise in strong support of H.R. 5835, and I yield myself such time as I may consume.

Mr. Speaker, having moved H.R. 5835, as amended, the Veterans Identity Credit Security Act of 2006, I, along with Ranking Member LANE EVANS and Acting Ranking Member BOB FILNER, Chairman DAVIS, and Ranking Member WAXMAN of the Committee on Government Reform, Chairman WALSH and Ranking Member EDWARDS on the Appropriations Subcommittee on Military Quality of Life and Veterans Affairs, and other members of this body introduced this legislation on July 19, 2006.

Since 2000, the Veterans' Affairs Committee and our subcommittees have held 16 hearings on information technology at the Department of Veterans Affairs, and as a subset, information security issues. These hearings have covered a variety of IT issues, including the budget, organization, authorities, actions VA has taken regarding its IT programs, and of course information security.

Last year, the House passed H.R. 4061 to address problems in IT at the VA. The Senate and the administration can best be described as having stiff-armed us in our proposals to centralize the IT architecture at the VA, opting for more of what they call now a federated model, or what I will also refer to as an incremental approach. That is how they wanted to proceed. Then bad things happened.

This summer, we held 8 hearings in response to the May 3 theft of a loaned lap-top belonging to the VA that held the sensitive personal data of 26.5 million veterans and 2.2 million Guard and Reserve component servicemembers and families. We heard from 23 witnesses during our hearings. These witnesses included the VA's Secretary, the Inspector General, the General Counsel, as well as others from academia, the Government Accountability Office, and experts in data security, information technology management, and identity theft.

Mr. Speaker, I applaud Secretary of Veterans Affairs Jim Nicholson for his stated commitment to making the VA the gold standard in information security. H.R. 5835, as amended, will provide the Secretary with some of the tools needed to make the VA that gold standard and set an example for the Federal Government.

H.R. 5835, as amended, provides the chief information officer the authority to enforce information security in the Department. It also requires a monthly briefing to the Secretary on VA's compliance with the Information Security Management Act of 2002, which we refer to as FISMA.

Mr. Speaker, Chairman TOM DAVIS of the Committee on Government Reform and I have worked together cooperatively, and our staffs, on a provision in the bill, and the Committee on Government Reform has waived consideration of H.R. 5835. Included in this bill is a part of Chairman DAVIS' work product, and I want to thank him for his cooperation, along with Mr. WAXMAN.

I would, in addition, also like to thank Chairman MIKE OXLEY of the Committee on Financial Services, who has waived consideration on this bill, and the committee will continue to work with these two committees on this legislation as we move forward with the Senate.

Mr. Speaker, the letters that I have here in my hand between the two committees and the Veterans' Affairs Committee regarding H.R. 5835, in which they have waived jurisdiction, are submitted as follows for the CONGRESSIONAL RECORD.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON VETERANS' AFFAIRS,
Washington, DC, September 12, 2006.

Hon. TOM DAVIS,
Chairman, House Committee on Government Reform, Washington, DC.

DEAR CHAIRMAN DAVIS: I am writing regarding your committee's jurisdictional interest in H.R. 5835, the Veterans Identity and Credit Security Act of 2006, and would appreciate your cooperation in waiving consideration of the bill by the Committee on Government Reform in order to allow expedited consideration of the legislation next week under suspension of the rules.

I acknowledge your committee's jurisdictional interest in section 2 of H.R. 5835, as ordered reported by the Committee on Veterans' Affairs. Any decision by the Committee on Government Reform to forego further action on the bill will not prejudice the Committee on Government Reform with respect to its jurisdictional prerogatives on this or similar legislation. I will support your request for an appropriate number of conferees should there be a House-Senate conference on this or similar legislation.

Finally, I will include a copy of this letter and your response in the Congressional Record when the legislation is considered by the House.

Thank you for your assistance.

Sincerely,

STEVE BUYER,
Chairman.

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, DC, September 12, 2006.

Hon. STEVE BUYER,
Chairman, House Committee on Veterans Affairs, Washington, DC.

DEAR STEVE:, On July 20, 2006, the House Veterans' Affairs Committee reported H.R. 5835, the ''Veterans Identity and Credit Security Act of 2006.'' As you know, the bill includes provisions within the jurisdiction of the Committee on Government Reform including Section 2 of the bill regarding federal agency data breach notification amendments under the Federal Information Security Management Act (FISMA).

In the interest of moving this important legislation forward, I agreed to waive sequential consideration of this bill by the Committee on Government Reform. However, I do so only with the understanding that this procedural route would not be construed to prejudice the Committee on Government Reform's jurisdictional interest and prerogatives on this bill or any other similar legislation. I understand this will not be considered as precedent for consideration of matters of jurisdictional interest to my Committee in the future.

I respectfully request your support for the appointment of outside conferees from the Committee on Government Reform should this bill or a similar bill be considered in a conference with the Senate. Finally, I request that you include this letter and your response in the Congressional Record during consideration of the legislation on the House floor.

Thank you for your attention to these matters.

Sincerely,

TOM DAVIS.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON FINANCIAL SERVICES,
Washington, DC, September 26, 2006.

Hon. STEVE BUYER,
Committee on Veterans Affairs,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN, I am writing to confirm our mutual understanding with respect to the consideration of H.R. 5835, the Veterans Identity and Credit Security Act of 2006. This bill was introduced on July 19, 2006, and referred to the Committees on Veterans Affairs and Government Reform. I understand that committee action has already taken place on the bill and that floor consideration is likely in the near future.

Portions of section 4 of the bill as reported involve remedies for breaches in data security. Some of these remedies, such as a credit security freeze, fall within the jurisdiction of this Committee and could have caused the referral of this bill to the Committee on Financial Services. However, given the importance and timeliness of this bill, and your' willingness to work with us regarding these issues as the legislative process continues, proceedings on this bill in this Committee will not be necessary. However, I do so only with the understanding that this procedural route should not be construed to prejudice the jurisdictional interest of the Committee on Financial Services on these provisions or any other similar legislation and will not be considered as precedent for consideration of matters of jurisdictional interest to my committee in the future. Furthermore, should these or similar provisions be considered in a conference with the Senate, I would expect members of the Committee on Financial Services be appointed to the conference committee on these provisions.

Finally, I would ask that you include a copy of our exchange of letters in the Congressional Record during the consideration of this bill. If you have any questions regarding this matter, please do not hesitate to call me. I thank you for your consideration.

Yours truly,

MICHAEL G. OXLEY,
Chairman.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON VETERANS' AFFAIRS,
Washington, DC, September 26, 2006.

Hon. MICHAEL G. OXLEY,
Chairman, House Committee on Financial Services, Washington, DC.

DEAR CHAIRMAN OXLEY, Thank you for your recent letter regarding your committee's jurisdictional interest in H.R. 5835, the Veterans Identity and Credit Security Act of 2006. I appreciate all of your efforts to expedite consideration of this important legislation.

I acknowledge your committee's jurisdictional interest in portions of section 4 of the bill as ordered reported by the Committee on Veterans' Affairs, which involve remedies for breaches in data security. I further acknowledge that some of these remedies, such as a credit security freeze, fall within the jurisdiction of your committee, and could have been referred to the Committee on Financial Services. I appreciate your cooperation in allowing speedy consideration of the legislation. We will continue to work with your Committee regarding these issues as the legislative process continues.

I agree that your decision to forego further action on the bill will not prejudice the Committee on Financial Services with respect to its jurisdictional prerogatives on this or similar legislation. I will support your request for an appropriate number of conferees should there be a House-Senate conference on this or similar legislation.

Finally, I will include a copy of your letter and this response in the Congressional Record when the legislation is considered by the House. Thank you for your assistance.

Sincerely,

STEVE BUYER,
Chairman.

Mr. Speaker, H.R. 5835, as amended, requires notification to Congress and individuals in the event of a data breach. The bill would require the VA to conduct a data breach analysis, and if the Secretary deems necessary, to provide credit protection at the request of affected individuals. This protection may include a credit freeze, identity theft insurance and/or credit monitoring.

The bill also requires a report on the feasibility of using an independent number for identification in lieu of the Social Security Number.

This bill also includes a scholarship and loan repayment program to provide the Secretary with a recruitment and retention tool to attract qualified people in the area of information technology and information security to work at the VA.

Mr. Speaker, I reserve the balance of my time.

Mr. FILNER. Mr. Speaker, I yield myself such time as I may consume.

As Chairman BUYER stated, a near catastrophe occurred in early May of this year when a lap-top containing 26 million names and data, Social Security data and some medical data, was stolen from a VA employee's home. Now, this theft of data was not just human error, it was not just an accident, it was not just bad luck. As Mr. BUYER had been pointing out for many years, this was a systemic problem, a problem of incredibly bad management of cyberinformation at the VA, a lack of cybersecurity, a lack of centralization of responsibility for cybersecurity, and it could have resulted in identity theft for millions of our Nation's veterans.

We were lucky. Apparently, the laptop was recovered before the names were stolen. Although I don't have 100 percent confidence in that judgment, that is what we think right now. But the Committee on Veterans' Affairs, under the leadership of Chairman BUYER, saw this as a wake-up call, a time to change failed policies, a time to change directions. Under the leadership of Chairman BUYER, the Committee on Veterans' Affairs took this wake-up call as an opportunity to change the way things were going, to change a backward culture, and to bring the VA into the 21st century.

Now, Mr. BUYER had been saying such things about the need for cybersecurity and the need for centralization for many years. I have to say, Mr. BUYER, that I admire your persistence and your lack of discouragement when people did not pay attention. We should have. But we are now, and we thank you for doing all that work at a time when people did not pay much attention.

I think you have, you have set up a model here in the bill that other Departments in the government should be looking at. You have set up a model where we can in fact say to the people who our government is serving, we are protecting your identity, we are protecting your data, we are making sure that if there is any breach of that, we will take these steps to make sure you don't have any losses, either material or psychological. And that was a real problem in the VA which you recognized.

When this data was stolen, there was incredible fear throughout the country, because the VA did not have the steps ready to take to assure the veterans that they would not suffer any material or other loss. So, Mr. BUYER, I thank you for working not only in a bipartisan manner, but bicameral and bicommittee. You brought everybody into the process.

The committee held hours and hours of hearings. We checked out all the expertise in the country. Our chairman, Mr. BUYER, brought expertise from all around the Nation. I think we took the role of oversight that is appropriate for every committee in this Congress, that is, we had a problem with the executive branch, we went to work to make sure that we had the knowledge, we had the information, we had the attention of the executive branch; and this bill is a result of that effort.

I think Mr. BUYER described what was in the bill. I just want to point out that it establishes data breach notification requirements, it makes substantive changes to how the VA addresses information technology, and it clarifies how the VA is to comply with the Federal Information Security Management Act of 2002.

□ 2200

Most importantly, it provides veterans with the tools that they can use immediately to protect themselves in the case of future data breaches. If a veteran's data is compromised, they can immediately request that a fraud alert be placed on their credit files for a period of 1 year, as well as a credit security freeze.

It also mandates that the VA undertake an independent analysis of any data breach, and if it is determined that a reasonable risk of misuse exists, then the VA will provide a range of remediation services, including making available data breach analysis, credit reports, credit monitoring services, and identity theft insurance.

Finally, and again, Mr. BUYER, your creativity here was very important, knowing that an agency like the VA, which does not have the background or information or expertise, you said let's create a scholarship fund so we can train people in this area and that the VA can fund and then draw on that new expertise to improve its services in the cybersecurity area.

So, again, I think this is a model for other agencies to look at, the way you looked at a problem and not only tried to solve it, but moved us forward with a real creative program of scholarship and loan forgiveness that I think will help students in our Nation and, of course, help our Federal Government.

The VA Secretary, Mr. Nicholson, has stated that the goal now is to make the VA the gold standard in data security. I hope he takes advantage of this bill to allow him to reach that goal.

I thank Chairman BUYER for the way he undertook the oversight, the bipartisan way we approached this bill, the drawing on all the Members for their ideas and their expertise, and I urge us all to support this bill.

Mr. Speaker, I reserve the balance of my time.

Mr. BUYER. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I will cherish the sincerity of the compliment from Mr. FILNER. I do not question his commitment nor his motive to the service of veterans in this country. I think members of the committee over the last 14 years have recognized that Mr. FILNER and I have had some real battles, but at the same time, when it comes to this particular issue on IT, there is no difference. We walk together in lockstep.

It is not just Mr. FILNER and I. It is the entire committee over the years we have taken this on, even when I chaired the oversight investigations. So I appreciate the commitment on both sides on improving the IT infrastructure.

I also want to compliment the Government Reform Committee, because they have taken this issue on over the years.

Mr Speaker, I yield 4 minutes to the gentleman from Virginia (Mr. TOM DAVIS), chairman of the Government Reform Committee, and thank him for his cooperation in working with our committee. He introduced his own bill on notification provisions. He worked with us and waived jurisdiction. We incorporated that in our bill.

Mr. TOM DAVIS of Virginia. Chairman BUYER, I thank you and Mr. FILNER for your leadership on this.

Secure information is the lifeblood of effective government policy and management, yet Federal agencies continue to hemorrhage vital data. Recent losses of personal information compel us to ask, what is being done to protect the sensitive digital identities of millions of Americans, and how can we limit the damage when personal data goes astray?

As we all now know, a Department of Veterans Affairs employee reported the theft of computer equipment from his home, equipment that stored more than 26 million records containing personal information. VA leadership delayed acting on the report for almost 2 weeks while millions were at risk of serious harm from identity theft and the agency struggled to determine the exact extent of the breach.

But this is only one in a long string of personal information breaches in the public and private sectors, including financial institutions, data brokerage companies, and academic institutions. Just last week, we learned the Census Bureau cannot account for 1,100 laptops issued to employees. These breaches illustrate how far we have to go to reach the goal of strong, uniform government-wide information security policies and procedures.

On our committee, we focused on government-wide information management security for a long time. The Privacy Act and the E-Government Act of 2002 outline the parameters for the protection of personal information. These recent incidents highlight the importance of establishing and following security standards for safeguarding personal information. They also highlight the need for the proactive security breach notification requirements for organizations, including Federal agencies, that deal with sensitive personal information.

Congress has been working on requirements for the private sector, but Federal agencies present unique requirements and challenges, and these incidents demonstrate that we need to strengthen laws and rules protecting personal information held by Federal agencies.

Given the VA incident, and in order to get a more complete picture of the problems before pursuing legislation, our Committee sent a request to every Cabinet agency seeking information about data breaches.

The results are in, and they are troubling. We have learned there has been a wide range of incidents involving data loss or theft, privacy breaches and security incidents. In almost all of these cases, Congress and the public would not have learned of such events unless we had requested the information. This history of withholding incidents has to stop.

Our committee bill, which has been incorporated as a manager's amendment in section 2, requires that timely notice be provided to individuals whose sensitive personal information could be compromised by a breach of data security at a Federal agency.

Despite the volume of sensitive information held by agencies, until now there has been no requirement that people be notified if their information is compromised. Under this legislation, the administration must establish practices, procedures, and standards for the agencies to follow if sensitive personal information is lost or stolen and there is reasonable risk of harm to an individual; and we provide a clear definition of the type of sensitive information we are trying to protect. We also give the agency CIOs the authority when appropriate and authorized to ensure that agency personnel comply with the information security laws that are already on the books.

Finally, we ensure that costly equipment containing potentially sensitive information is accounted for and secure. Half of the lost Census Bureau computers simply weren't returned by departing or terminated employees. The agency did not track computer equipment, nor were employees held accountable for failing to return it. This is taxpayer-funded equipment containing sensitive information, and we have to know who has it at all times.

Each year our committee releases information security score cards. This year the VA earned an F, the second consecutive year and fourth time in the past 5 years the Department received a failing grade, and the government overall got a D-plus.

Our Federal Government has sensitive personal information on every citizen, health records, tax returns, military records. If our government can't secure this information, who can? We need to ensure the public knows when its sensitive personal information has been lost or compromised in some way.

I again want to commend my colleagues, Chairman BUYER, Ms. PRYCE, Mr. SWEENEY, Mr. FILNER, all who recognize the importance of securing personal information held by agencies. I appreciate their work in supporting this issue. The provisions we have included in this bill are a great first step. If new policies and procedures are not forthcoming quickly or if they fail to have the teeth to get the job done, we will revisit the matter.

Mr. FILNER. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, again, to have the chairman of another committee testify to working together is really I think a good model. So thank you again, Mr. Chairman.

Mr. Speaker, I yield such time as she may consume to the gentlewoman from South Dakota (Ms. HERSETH), the ranking member of our Economic Opportunities Subcommittee of the VA committee, a lady who has left much of her fingerprints on this bill. We thank you for your expertise, your real ability to stick to the issues here.

Ms. HERSETH. Mr. Speaker, I want to thank Mr. FILNER for yielding. I would like to congratulate both Chairman BUYER and Ranking Member Filner for their hard work in bringing this urgently needed bill to the House floor. I appreciated working with them both in the many oversight hearings to review the VA's information technology management system.

The Veterans Identity and Credit Security Act is the result of judicious bipartisan work by members and staff of the House Veterans' Affairs Committee, working closely with those on the Government Reform Committee; and it is an important step towards safeguarding the personal information of our Nation's veterans.

Now, I share the frustration of my colleagues regarding the repeated failures of the VA's information technology management and the theft in May of the personal data of as many as 26.5 million veterans and servicemembers from a VA employee's home.

While we are all relieved the laptop containing this data has been recovered and authorities have found no evidence that the data has been accessed, the data breach raised serious concerns about the VA's information security. It is clear that we dodged a bullet.

Perhaps the most frustrating aspect of the security breach was the previous recommendations and warnings by the General Accounting Office and the VA's Inspector General were not given adequate consideration. The Department's inexcusable and unacceptable inaction was disrespectful to the brave men and women who serve the country.

As my colleagues have outlined, the Veterans Identity and Credit Security Act would require the VA to report to Congress after any data theft and to provide credit monitoring and fraud remediation services to affected individuals. The bill creates an Under Secretary for Information Services, sets conditions of contracting with the VA for work dealing with sensitive personal information, and establishes a scholarship program for students pursuing doctorates in information technology, security or computer engineering.

I believe these important changes to the VA's information technology management structure are essential to better protecting the personal information of our Nation's veterans and their families. While there is no perfect solution, given the magnitude of this problem, not only for the VA but so many other Federal agencies, as the gentleman from Virginia just described, this legislation is an important step in the right direction.

I encourage my colleagues to support it.

Mr. BUYER. Mr. Speaker, the gentleman from South Carolina has requested 2 minutes of me, and I have great fear that the slowest talking man from the First District of South Carolina may not make the mark. But let's see how he does.

I yield 2 minutes to the gentleman from South Carolina (Mr. BROWN), the chairman of the Health Subcommittee of the Committee on Veterans' Affairs.

Mr. BROWN of South Carolina. Mr. Speaker, I thank my friend, the chairman, for yielding me this time; and I hope I can make it in 2 minutes.

This is an important issue, one which the committee has addressed not only by this legislation, but also through hearings and meetings of members of the committees, officials from the VA, and representatives of our Nation's veterans organizations.

As chairman of the Committee's Subcommittee on Health, I led the committee's effort to understand the health-related impact of the recent loss of computers by the Veterans Administration. While this summer's computer loss regrettably saw the theft of VA data, this incident did not see the security of veterans health records compromised.

Indeed, recent events, such as the VA's response to Katrina, have shown the value of electronic medical records. During the aftermath of that disaster, VA doctors and nurses were able to treat without interruption patients transferred from VA facilities in New Orleans because of the VA's reliance on electronic medical records. All patient records were backed up, secured, transported and were back online and available almost immediately.

That said, we should not let the benefits of portable electronic records of any kind conflict with the need to keep them secure. Medical records contain a great deal of confidential personal information; and if those records get in the hands of the wrong people, it would pose a real problem and even in some cases, perhaps a national security risk.

For that reason, Congress needs to remain vigilant in order to ensure against the loss of all information by the VA. The VA itself needs to be proactive in maintaining the integrity of the health records. Lastly, our soldiers and their families need to continue to feel secure with VA having guardianship over those records.

In closing, I thank the chairman and the ranking member for their leadership on this issue and for introducing this important legislation. I urge all Members to support H.R. 5835.

Mr. FILNER. Mr. Speaker, I reserve the balance of my time.

Mr. BUYER. Mr. Speaker, I am so proud of my friend from South Carolina for delivering those remarks within the limits of time.

Mr. Speaker, I yield 2 minutes to the gentleman from Arkansas (Mr. BOOZMAN).

Mr. BOOZMAN. Mr. Chairman, I want to congratulate you for your leadership and really appreciate all the hard work. This has been a difficult thing to get to the floor. Also I want to thank Mr. FILNER and Ms. HERSETH and again the staffs on both sides that have worked so very, very hard to, like I say, get this thing done.

I rise in strong support of H.R. 5835, and I would like to highlight section 7 of the bill. This section would create a scholarship and debt reduction program at VA to encourage recruitment of new personnel with Ph.D.s in information security, computer engineering or electrical engineering from an accredited institution of higher learning. This is so we can attract and secure the best talent possible at the VA's IT department.

This section would allow the Secretary to award scholarships or repayment of education debts to future VA employees. The scholarships would not exceed $200,000, or $50,000 per year, per person. Debt reduction payments would not exceed $82,500 over a total of 5 years of participation, or $16,500 per year in the program. The recipients would also be required to agree to a period of obligated service at the Department of not less than 2 years for every 1 year of tuition paid.

This is a great way to attract talented people at the VA. I urge my colleagues to support H.R. 5835.

□ 2215

Mr. BUYER. I appreciate the chairman's contribution to the bill. He chairs the Economic Opportunity Subcommittee on Veterans Affairs.

At this time, I yield 2 minutes to Mr. MURPHY of Pennsylvania, who also worked with us on the bill. He had his own bill, H.R. 6109, dealing with encryption; and we worked with the gentleman. We have three legacy platforms which are basically older operating systems. We were not able to achieve everything the gentleman has been seeking, but I want to appreciate the gentleman's sincerity and his effort and want to continue to work with the gentleman.

Mr. MURPHY. Mr. Speaker, I am in support of H.R. 5835 and commend the distinguished chairman for his hard work for veterans.

We all know veterans deserve the best from the Federal Government following their service. Unfortunately, on two separate occasions there were some major breaches which raised the risk of identity theft and fraud. In May, the VA announced a laptop computer containing personal information of 26 million veterans and spouses had been stolen; and, in August, a desktop with personal and health information of 38,000 veterans was stolen from a subcontractor performing insurance collections for VA medical centers in Pittsburgh and Philadelphia.

These losses are totally unacceptable. Identity theft touches the lives of more than 10 million Americans per year, and our veterans deserve better protection of their records. The bill before us would provide better protections, and these are important steps, and we should support the underlying bill.

In addition to H.R. 5835, I introduced last week H.R. 6109, the Stop Endangering the Records of Veterans, or the SERV Act. This bill would require the VA to physically secure and encrypt all veterans' personal records held by the Department. The VA announced in August that it will add enhanced encryption systems to all the Department's laptop and desktop computers. Today may not be the day for Congress to pass the requirements of H.R. 6109, since a great deal of technical work is currently taking place to define how these encryptions should take place with the system, but I look forward to joining Chairman BUYER and my colleagues in energetic oversight of the VA's implementation of encryption standards on this data.

Mr. Speaker, America's veterans have given blood, sweat, and tears for our Nation from the world wars to the current operations in Iraq and Afghanistan. They have earned peace of mind when it comes to their critical personal information. Today, the House is helping to ensure the mistakes of this year will not happen again.

Again, I commend the leadership of Chairman BUYER and all the members of the Veterans Committee, and I urge my colleagues to support H.R. 5835.

Mr. BUYER. At this time, I would like to yield 1 minute to the gentleman from San Diego, California (Mr. BILBRAY), who helped us work on the provisions of the bill.

Mr. BILBRAY. Mr. Speaker, I rise in support of the bill and would like to thank the chairman of the committee for this legislation, and I would like to thank the ranking member, my old friend, Mr. FILNER from San Diego.

Let me just say, sincerely, I think this is what America wants, this is what our veterans need. I think it is a great bipartisan cooperative effort.

The fact is that there are challenges under today's new technology opportunities we have that can be used or abused, and hopefully this bill will be able to tighten up the procedures to make sure we reflect those new realities.

Mr. Speaker, I in no little way want to praise both sides of the aisle for doing what is right for our veterans. Hopefully, we have been able to avoid a major problem in the past and with this legislation will make sure that no major problem occurs.

The identity and the personal records of our veterans are cherished possessions that we hold in the Federal Government, and we want to maintain those for the veterans and not allow it to leak out.

I thank very much both the ranking member but, most importantly, the chairman of the full committee.

Mr. BUYER. Mr. Speaker, I reserve the balance of my time.

Mr. FILNER. Mr. Speaker, again, I think this is an incredibly good bill. It shows the way we ought to work as a Congress and as a committee. Again, I thank one more time Mr. BUYER for his leadership and urge passage of the bill.

I yield back the balance of my time.

Mr. BUYER. Mr. Speaker, I want to thank you for allotting the time for us to bring this bill to the floor. This is bipartisan legislation. It reflects proposals introduced in this Chamber over the past months. I thank the Members and staff who contributed to this legislation. I am especially grateful for the support of LANE EVANS and BOB FILNER in moving this bill through the committee and to the floor.

I want to thank Chairman DAVIS and Ranking Member WAXMAN of the Government Reform Committee in our work on the FISMA component of the bill. I also would like to thank Chairman OXLEY and Ranking Member FRANK of the Financial Services Committee for their assistance in moving this bill to the floor, as well as the Appropriations Subcommittee on Military Quality of Life and Veterans Affairs Chairman WALSH and Ranking Member EDWARDS, and to recognize again that information security is crucial to our veterans and have provided valuable support for this legislation.

I also commend Mr. BILIRAKIS and Mr. STRICKLAND, the chairman and ranking member of the Subcommittee on Oversight and Investigations, for their oversight of IT at the VA. I am indebted to the chairmen and ranking members of the committee's Subcommittees on Health, Disability Assistance and Memorial Affairs and Economic Opportunity for their help in reviewing the VA's data security and coming up with this legislation.

Mr. Speaker, several Members introduced legislation after the May 3 loss, including Representatives HOOLEY, SALAZAR, and BILBRAY from the Committee on Veterans Affairs. Representatives BLACKBURN, ANDREWS, DRAKE, CAPITO, and GRANGER also introduced legislation, and all of this legislation was taken into account to create this product that has come to the floor. So this is a pretty good work product, to also include that of the gentleman from Pennsylvania.

I also want to thank the Subcommittee on Oversight and Investigations; the staff director, Art Wu; and minority staff director, Lynn Sistek, for their work on this legislation.

Mr. Speaker, I urge my colleagues to support our veterans by passing H.R. 5835, the Veterans Identity and Credit Security Act of 2006. This legislation will safeguard the sensitive personal information of veterans, and help lay the groundwork for a national solution

Ms. WATERS. Mr. Speaker, I rise in support of H.R. 5835, the Veterans Identity and Credit Security Act.

Earlier this year, millions of veterans saw their economic security threatened when several VA computers were stolen from a Veterans Administration (VA) employee's home. While it appears that no veteran was a victim of ID theft, the VA was ill-prepared to deal with the lost of this highly personal and confidential information.

While I am pleased to support this bill, which will help safeguard veterans' personal information in the future, I urge this Congress to immediately pass legislation that will protect all Americans from ID theft, not just our veterans. The threat of ID theft is too important to ignore any longer.

Data security is an issue that we have labored over for months, and while this will protect America's veterans from breaches of data security, the American public wants Congress to act to protect its private information as well.

As many of my colleagues have outlined during the debate today, this bill takes several steps to empower the VA to combat ID theft. It creates a new Office of the Under Secretary for Information Services within the Department. The bill also requires the VA to notify affected individuals when sensitive, personal information held by VA is lost, stolen, or otherwise compromised. In addition, the bill requires the VA to provide services to alleviate any loss those individuals might suffer, if the Secretary of VA determines there is a risk that the compromised information could be used in a criminal manner. Another important provision in the bill requires contractors to pay damages to VA if the compromised information was under the contractors' control. The combination of these provisions represents a well thought through piece of legislation.

Mr. Speaker, having ones identity stolen can unleash a lifetime of problems for its victims. It can impair buying a home, applying for jobs and loans as well as a host of other problems.

I am pleased to support this bill to help protect our veterans from these personal and economic pitfalls. I urge my colleagues to support this bill.

Mr. STEARNS. Mr. Speaker, I rise to support H.R. 5835, the Veterans Identity and Credit Security Act of 2006. I was deeply concerned that nearly 27 million veterans may have been affected by a data security breach of record proportions, that could have compromised sensitive, personal information. Twenty-six-and-a-half million veterans, and 2.2 million Guards, Reservists, and active duty servicemembers, were at risk. Fortunately, we recovered the stolen laptop and forensic analysis revealed the data was uncompromised. While it turned out that no veterans' information was jeopardized, it was a lesson in carelessness that cannot be repeated. We have learned from this incident what steps we must take to (a) change the organizational structure

and requirements at the VA, and (b) design a meaningful package of action items we will deliver for veterans should a breach ever occur again. Now we must implement them.

Unfortunately, data breaches like this highlight the need for legislation I have authored: H.R. 4127, the Data Accountability and Trust Act (DATA). This bill, which the Energy and Commerce Committee has passed, goes to the heart of this problem of the critical need to protect consumers' personal information. Let's fix this.

I thought, and Chairman BUYER agreed, that while we are instructing the VA when they must notify veterans, let's not limit ourselves to notification by ''snail mail''. I appreciate the Chairman's incorporating my language into H.R. 5835. The standard of business practice is—if a consumer or veteran in this case prefers—to communicate in writing by e-mail, because it is immediate and portable. What if a veteran is now in the Florida National Guard, serving in Iraq, and suffers a breach? We would not want him or her to wait for a hard copy letter to make its way. Secondary to providing better service to the veteran, this would save tremendous money to the VA, money better spent on veterans health care and services: I understand the May 2006 notification mailing cost the VA about $7 million.

Through both of my Committee seats, I will continue to take an active role in ensuring that veterans, and all consumers, feel confident and secure about their financial and personal information. And, thank you, Chairman BUYER, for your steadfast leadership on this issue for years.

Mr. BILIRAKIS. Mr. Speaker, I ask unanimous consent to revise and extend my remarks.

Mr. Speaker, I rise in strong support of H.R. 5835, the Veterans Identity and Credit Security Act of 2006, as amended, and thank Chairman BUYER for his leadership in bringing this legislation to the floor. I also want to thank my colleagues from other Committees and across the aisle for the bipartisan effort that brought this bill to the floor. This is an important piece of legislation that aims to improve information security at the Department of Veterans Affairs (VA), and may set VA as an example for other federal departments and agencies.

H.R. 5835, as amended, provides the tools for VA to improve information security and strengthens the role of the Chief Information Officer (CIO). The legislation, requires the Secretary to provide the CIO with the authority over VA information technology (IT) to include information security, personnel, resources, and infrastructure. These authorities include oversight of the activities, policies, processes, and systems of VA IT.

Last October, as Chairman of the Subcommittee on Oversight and Investigations, I joined Chairman BUYER, Ranking Member EVANS, Subcommittee on Oversight and Investigations Ranking Member STRICKLAND and other distinguished Members to introduce H.R. 4061, the Department of Veterans Affairs Information Technology Management Improvement Act, to centralize the authority of the CIO. Last November, the House unanimously passed H.R. 4061 with a vote of 408–0. I remember Chairman BUYER standing on this floor, sharing the failures of VA IT projects and the millions of dollars spent on major IT programs that have failed to assist in making the delivery of benefits to veterans faster, safer, and more efficient. I stand here today because of another VA failure in IT, with another piece of legislation to reform VA IT and ask members to unite and show support for our veterans by passing H.R. 5835, as amended.

Since 2000, there have been 16 hearings of the House Committee on Veterans' Affairs and its Subcommittees on VA IT. This summer alone the Committee on Veterans' Affairs held eight hearings on IT and information security, two of which were at the Subcommittee level. The House Committee on Veterans Affairs has been anything but lax in its review of VA IT, and I am confident that oversight of VA IT will continue following my retirement.

It has been an honor to serve in this body and as a member of the House Committee on Veterans' Affairs for the past 24 years, and passing H.R. 5835, would be another way for me to honor and protect the veterans I have served during my time in Congress. I urge my colleagues to vote in favor of H.R. 5835, as amended.

Mr. MICHAUD. Mr. Speaker, I rise today in strong support of H.R. 5835, the Veterans Identity and Credit Security Act.

Earlier this year, VA experienced a major breach in the data security of millions of veterans. Their very identities and financial lives were put at risk. Thanks to the efforts of law enforcement, and a great deal of luck, this breach did not turn into a disaster.

While for many, this breach came as a surprise, the reality is that VA leadership has been warned repeatedly that VA's information security program is weak and could be compromised. The Veterans Affairs Committee has been calling on the VA to make changes. The VA's Inspector General and the GAO have issued report after report raising significant concerns about weaknesses in the security of VA's data and information systems. The sad reality is that this data breach, while larger than any other, was not unique.

We do a disservice to the men and women who have served our Nation and their families if we allow VA's information security policies and practices to continue as the status quo.

H.R. 5835 moves the VA toward greater IT security. It will create a clear line of responsibility through the Office of the Under Secretary for Information Security. It will put in place policies to improve IT security, notification and remediation. In cases of identity theft, this bill will help veterans recover their identities and their lives.

I also believe that the provisions in this bill supporting further education in IT security are innovative and extremely important for addressing this challenge in the future.

I want to congratulate the members of the Veterans Affairs Committee, especially Chairman BUYER and Mr. FILNER, for working quickly to move this important legislation forward.

I urge my colleagues to support this bill.

Mr. SWEENEY. Mr. Speaker, I rise in strong support of the Managers Amendment to H.R. 5835, the Veterans Identity and Credit Security Act of 2006.

Over the past 5 months, data security incidents at the Department of Veterans Affairs, State Department and Census Bureau have raised concern over the use of secure data at these and other Federal agencies.

The VA learned that an employee took home electronic records of 26.5 million veterans and 2.2 active-duty soldiers from the VA, which he was not authorized to do.

A hacker at the State Department gave thieves access to a finite amount of information, access to data and passwords.

The census bureau lost track of over 1,000 laptops, some of which contained sensitive personal information.

Americans secure information was put at extreme risk and raised concerns about data security in the Federal Government to a whole new level.

GAO reports released in July 2005 and again in March of 2006, revealed despite progress in implementing Federal requirements to protect information and systems, the 24 major Federal agencies' experienced continued pervasive weaknesses in information security policies and practices. Their flaws put Federal operations, citizens personal financial data and assets at risk of fraud, misuse, disclosure and destruction.

That is why I introduced H.R. 5820, the Federal Agency Data Privacy Protection Act, legislation that adds security measures to all Federal agencies data usage and administration. This manager's amendment includes a number of provisions included in my legislation.

It is important that we protect the sensitive information Americans provide to us so that we can assist them and we must provide the best possible responses to personal information being placed at risk. It is critical that we provide proper protections to individuals who may be affected by these thefts.

This amendment also extends the definition of what constitutes secure data so that we can provide the best protection for all personal information used by Federal agencies.

Americans place their trust in the Federal Government to protect the information they provide. In this age of technology, we have an obligation to protect that information and serve the people of this Nation. I urge my colleagues support on this amendment.

Ms. JACKSON-LEE of Texas. Mr. Speaker, I rise today to support H.R. 5835, to amend Title 38, United States Code 106–348, to improve information management within the Department of Veterans Affairs, and for other purposes.

In June, the Defense Department revealed that the personal information of about 2.2 million National Guard and Reserve troops was stolen from a government employee's house. In August of this year, the Department of Veterans Affairs reported that a subcontractor's missing laptop contained personal information of some 16,000 veterans and their families who were treated in VA medical centers in Pittsburgh and Philadelphia.

Even more astonishing is the fact that earlier this month, the Commerce Department reported that 1,100 of its laptops were missing from the last five years, some containing personal data from the U.S. Census Bureau.

These incidences of missing sensitive personal data are no small matters of concern. All of us as citizens of this great country expect to enjoy the privilege of privacy when it comes to our often sensitive personal data. As we are all well aware, such information can be easily mishandled and misused to the detriment of anyone who becomes so-victimized.

This reason alone is why it is crucial to provide sufficient safeguards to prevent or at the very least minimize the degree to which the privacy of sensitive personal data of our veterans as well as all the citizens of this country may become compromised.

H.R. 5835 provides safeguards to: Amend FISMA (Federal Information Security Management Act) to authorize the Director of OMB to establish data breach policies for agencies to follow in the event of a breach of data security involving the disclosure of sensitive personal information and which harm to an individual could reasonably be expected to result; Amend FISMA to clarify authority of Chief Information Officer to enforce data breach policies and develop and maintain IT inventories; Amend FISMA to define sensitive personal information as ''any information about an individual maintained by an agency, including: education, financial transactions, medical history, criminal or employment history; information that can be used to distinguish or trace the individual's identity, including name, Social Security number, date and place of birth, mother's maiden name, or biometric records; or any other personal information that is linked or linkable to the individual;

Create the position of Under Secretary for Information Services in the VA and mandates that this individual serve as the VA's CIO;

Mandate that the office of the Under Secretary for Information Services shall consist of the three Deputy Under Secretaries (at least one of whom is to be a career employee);

Call for the VA to ensure that the CIO has the authority and control necessary to execute responsibilities under FISMA and requires an annual FISMA compliance report to be submitted to the Committees on Veterans' Affairs of the House and Senate, the House Government Reform Committee, and the Senate Homeland Security and Governmental Affairs Committee; it also requires a monthly report from the VA CIO to the VA Secretary regarding compliance deficiencies; and to require immediate notification by the CIO to the VA Secretary of any data breach, and notice by the VA to the Director of OMB, VA IG, and if appropriate, to the FTC and Secret Service;

Require quarterly reports from the VA to the Committees on Veterans' Affairs of the House and Senate on any data breach that occurred in the previous quarter and to also require prompt notice in the event of a significant data breach;

Require the VA to undertake, as soon as possible after a data breach, an independent risk analysis (conducted by a non-VA entity). The Secretary shall then make a determination, based upon this analysis, if there exists a reasonable risk for potential misuse of the compromised data. If the Secretary does determine that this potential exists, then the VA is required to provide credit protection services. In the event of any data breach, the VA shall notify all affected individuals of the breach and inform them that they may request, at no charge, a fraud alert and a credit security freeze for a period of one year. The notification is to clearly spell out the advantages and disadvantages to requesting these actions;

Require the VA to provide credit protection services, including data breach analysis, credit monitoring services and identity theft insurance, to covered individuals (defined as individuals whose sensitive personal information is involved in a data breach, on or after August 1, 2005 for which the Secretary determines a reasonable risk exists for the potential misuse of the sensitive personal information). Authorizes the VA to contract with other government agencies and credit reporting agencies to provide these services;

Require that when the VA enters into a contract that the contractor shall not compromise any sensitive personal information. In the event of a breach, the contractor shall pay liquidated damages (which will then be used by the VA to provide credit protection services);

Require the VA to submit a report not later than 180 days after enactment concerning the feasibility of using Personal Identification Numbers for identification purposes in lieu of Social Security numbers;

Require the President to nominate the Under Secretary for Information Services and the VA to appoint the Deputy Under Secretaries within 180 days of enactment. Requires a report on the progress of the nomination and appointments every 30 days.

All of these measures are essential pieces to ensuring that the privacy of personal sensitive data of all of our citizens is not compromised. We are far behind in taking action to ensure that integrity of information in this nation. This bill is an important first step.

I urge my colleagues to support this resolution.

Mr. WAXMAN. Mr. Speaker, I support the goal of H.R. 5835 to strengthen security of personal data held by the Government, but believe that more should be done. For the Department of Veterans Affairs, this bill provides more training for employees on privacy issues, independent risk analysis of data breaches, credit freezes for persons whose data has been compromised, and more. This is an important step in light of recent data losses at the VA.

But the detailed requirements in this bill only apply to the Department of Veterans Affairs. For the rest of the Government, none of this is required, even though our committee's inquiries have uncovered serious breaches in other Federal agencies. For example, the Department of Commerce recently reported the loss of more than 1,000 laptop computers, some containing census information. To protect the privacy of personal information, we should require increased training, accountability, and reporting in all Federal agencies, not just the VA.

I am also concerned about the procedures under which this bill has come to the floor. Although primarily a VA bill, this bill also includes amendments to the Federal Information Security Management Act, FISMA, a government-wide law, in the jurisdiction of the Committee on Government Reform. Some of these provisions were in the reported version of this bill, and some were just added by amendment today from a bill introduced yesterday. None of these government-wide provisions were considered in the Committee of Government Reform.

H.R. 5835 now includes 2 different definitions of ''sensitive personal information''—one applying to the entire government under FISMA, and another applying to the Department of Veterans Affairs. Had this bill proceeded through the regular committee process, inconsistencies like this could have been resolved and a clearer, more comprehensive bill reported to the floor. I hope that Congress will consider additional legislation to clarify the patchwork of laws and regulations currently in place and extend stronger data security requirements to the entire Federal Government.

Mrs. JO ANN DAVIS of Virginia. Mr. Speaker, although the Rules of the House of Representatives do not allow me to co-sponsor H.R. 5835, the Veterans Identity and Security Act of 2006, I wish to express my full support for this bill. My district is home to tens of thousands of veterans from every branch of the military, and this legislation will be extremely helpful to my constituents. The recent loss of data affecting over 26.5 million current and former service members was extremely unfortunate, and it became clear that the Department's data security and notification practices needed an overhaul. I believe this legislation will enable the Department of Veterans Affairs to better protect the personal identification data of those who have served and are serving our country, and I am pleased that we are taking steps to prevent these incidents in the future.

As our country increasingly relies on electronic information storage and communication, it is imperative that our Government amend our information security laws accordingly. This legislation will help in this effort, and I am wholeheartedly supportive.

Mr. BUYER. Mr. Speaker, I yield back the balance of my time and urge all Members to support this legislation.

The SPEAKER pro tempore (Mr. BISHOP of Utah). The question is on the motion offered by the gentleman from Indiana (Mr. BUYER) that the House suspend the rules and pass the bill, H.R. 5835, as amended.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

GENERAL LEAVE

Mr. BUYER. Mr. Speaker, I ask unanimous consent that all Members have 5 legislative days in which to revise and extend their remarks on H.R. 5835.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Indiana?

There was no objection.

ENCOURAGING ALL OFFICES OF THE HOUSE OF REPRESENTATIVES TO HIRE DISABLED VETERANS

Mr. EHLERS. Mr. Speaker, I move to suspend the rules and agree to the resolution (H. Res. 1016) encouraging all offices of the House of Representatives to hire disabled veterans.

The Clerk read as follows:

H. RES. 1016

Whereas the men and women of our armed forces play a central role in preserving our Nation's freedom;

Whereas disabled veterans have sacrificed greatly for their country;

Whereas one way for our Nation to repay its debt to those disabled veterans is to help disabled veterans return to their previous lifestyle;

Whereas Congress relies on knowledgeable staff to help formulate policy;

Whereas disabled veterans provide unique perspectives on a range of issues, especially regarding national security;

Whereas Members who are veterans or reservists have played a leading role throughout the history of Congress; and